



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ :

G06K 19/073

A1

(11) Numéro de publication internationale:

WO 99/49416

(43) Date de publication internationale: 30 septembre 1999 (30.09.99)

(21) Numéro de la demande internationale: PCT/FR99/00583

(22) Date de dépôt international: 16 mars 1999 (16.03.99)

(30) Données relatives à la priorité:

98/03471

20 mars 1998 (20.03.98)

FR

(81) États désignés: CA, CN, IN, JP, SG (US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)).

Publiée

Avec rapport de recherche internationale.

(71) Déposant (pour tous les États désignés sauf US): GEMPLUS S.C.A. [FR/FR], avenue du Pic de Bertagne, Parc d'Activités de Gémenos, Boîte postale 100, F-13881 Gémenos Cedex (FR).

(72) Inventeurs: et

(75) Inventeurs/Déposants (US seulement): FEYT, Nathalie [FR/FR]; Bâtiment 6, 20, rue du Lieutenant J.P. Meschi, F-13005 Marseille (FR). BENOIT, Olivier [FR/FR]; 22, rue Rastegue, F-13400 Aubagne (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

(54) Title: DEVICES FOR HIDING OPERATIONS PERFORMED IN A MICROPROCESSOR CARD

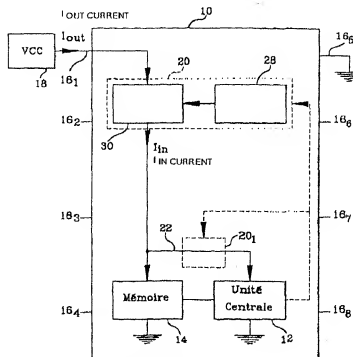
(54) Titre: DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS UNE CARTE A MICROPROCESSEUR

(57) Abstract

The invention concerns microprocessor cards and, in such cards, various devices for hiding operations performed in the card against fraudulent breaches by analysing the current consumed. The invention is characterised in that it consists in adding in the card a device (20) modifying the consumed current, either by averaging it by integration, or by adding thereto random values by a random signal generator (28) so as to hide the operations performed. In another embodiment, it consists in carrying out simultaneously an operation for making secure and writing in an EEPROM memory, the latter generating chaotic current variations which hide the operation to be made secure.

(57) Abrégé

L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte contre les intrusions frauduleuses par l'analyse du courant consommé. L'invention réside dans le fait d'ajouter dans la carte un dispositif (20) qui modifie le courant consommé, soit en le moyennant par une intégration, soit en lui ajoutant des valeurs aléatoires par un générateur de signaux aléatoires (28) de manière à masquer les opérations effectuées. Dans une variante, il est prévu d'effectuer simultanément une opération à sécuriser et l'écriture dans une mémoire EEPROM, cette dernière générant des variations de courant chaotiques qui masquent l'opération à sécuriser.



10. POWER CIRCUIT
14. MEMORY
12. CENTRAL PROCESSING UNIT

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brazil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Biélorus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						